Chapter 1

Weapons of Mass Destruction Civil Support Team Role and the Threat

In recent decades, the US has dealt with a series of asymmetric threats whose potential for lethality and political, economic, and psychological impact has increased over time. The most recent of these threats include terrorist bombings in New York City and Oklahoma City during the 1990s and the catastrophic destruction of the World Trade Center and significant damage to the Pentagon on 11 September 2001. The use of biological agents (such as anthrax) by terrorists also caused civilian casualties and contamination of US infrastructure (such as US mail distribution centers) in 2001. An adversary may not hesitate to use CBRNE or toxic industrial material (TIM) on a covert or overt basis to accomplish its objectives. Information technology and CBRNE materials have proliferated in recent years, making them more accessible to potential adversaries. The evolving threat has required that leaders and planners conduct assessments (during deliberate and crisis action planning) that analyze the impact of CBRNE on various courses of action (COAs) and the security of the US homeland. Based on the threat, the USG has undertaken measures to improve our nation's ability to respond to domestic and international-based terrorism. In June 1995, Presidential Decision Directive (PDD) 39, *US Policy on Terrorism*, delineated the responsibilities for federal agencies in combating terrorism, including domestic incidents. PDD 62, *Combating Terrorism*, issued in May 1998, further defined responsibilities for specific agencies. Both directives call for the establishment of robust, tailored, and rapidly deployable interagency teams that can conduct well-coordinated and highly integrated operations in response to the crisis generated by a terrorist attack (referred to as crisis management) and cope with the consequences that follow (consequence management [CM]).

CIVIL SUPPORT TEAM ROLE FOR SUPPORT OF HOMELAND SECURITY

1-1. In 1998, the Department of Defense (DOD) commissioned a "tiger team" to develop a strategic plan for integrating NG and reserve component (RC) support for response to attacks using WMD. The plan defined a future operational capability based on enhancing RC support to the civil authority in the US in managing the consequences of WMD terrorism. The subsequent approval of the plan by the Deputy Secretary of Defense (SECDEF) as *Defense Reform Initiative Directive Number 25*, together with the *Unified*

Command Plan for Fiscal Year 2000, the *Defense Planning Guidance (2002-2007),* the Chairman of the Joint Chiefs of Staff (CJCS) Contingency Plan 0500-98, and the *National Security Strategy* published in September 2002, charges DOD with the support of domestic CM.

1-2. Congress also directed the federal government to enhance its capability to deter, prevent, respond, and recover from terrorist attacks involving WMD and to provide direct support to the front line of local and state emergency response organizations. Beginning in Fiscal Year (FY) 1999, Congress and the DOD provided funding to train, organize, and equip NG WMD CSTs to develop a national military capability to meet the pressing demands of this emerging threat. The locations for the teams are chosen to maximize population coverage, minimize response times within a geographical area, and reduce the overlap with other teams' areas of responsibility. The distribution provides optimal response coverage for the majority of the US population; and over time, additional CSTs will be trained, authorized, and equipped.

1-3. The CSTs are designed to support the civil authorities in the event of a CBRNE emergency. The adjutant general (TAG) of a state employs the CST to support its home state's response (or another state's response) under the supported governor. As the "governor's 911 force for a WMD response," the CST contributes greatly to the overall national response capability for a CBRNE emergency consisting of local, state, and federal tiers.

1-4. The line between crisis management and CM is blurred. CSTs are state assets whose primary mission supports CM. They may support the crisis management mission (upon request by the appropriate authority) by performing tasks such as collecting an evidentiary sample and maintaining the chain of custody until it is delivered to applicable personnel; but this is secondary to their mission of identifying, assessing, advising, and assisting appropriate authorities at an incident site. They generally perform their mission at the state level. If an event is of the magnitude that the DOD becomes involved, the defense coordinating officer (DCO) may call upon a CST for its CM capabilities. Figure 1-1 shows the CM DOD response options. See Appendix B for information on CST utilization for different response options (such as a state emergency). The various CST response options may also generate questions on CST guidance for rules of engagement (ROE), and Appendix C provides guidance on the use of force.

1-5. The CSTs can respond from their respective home stations by air, maritime, and ground transportation to emergencies within a limited amount of time. Any response may require the use of rotary- or fixed-wing aircraft. Limited-capability CST equipment sets can be transported by helicopters; full-capability sets can be airlifted. The actual mode and speed of the deployment are determined by mission, enemy, terrain, troops, time available and civilian considerations (METT-TC).

PURPOSE

1-6. The purpose of the CST is to assess current and projected consequences and identify CBRNE agents and substances. The CST advises on response missions and assists with such measures as requests for additional support. Each team consists of 22 full-time Army and Air National Guardsmen and is

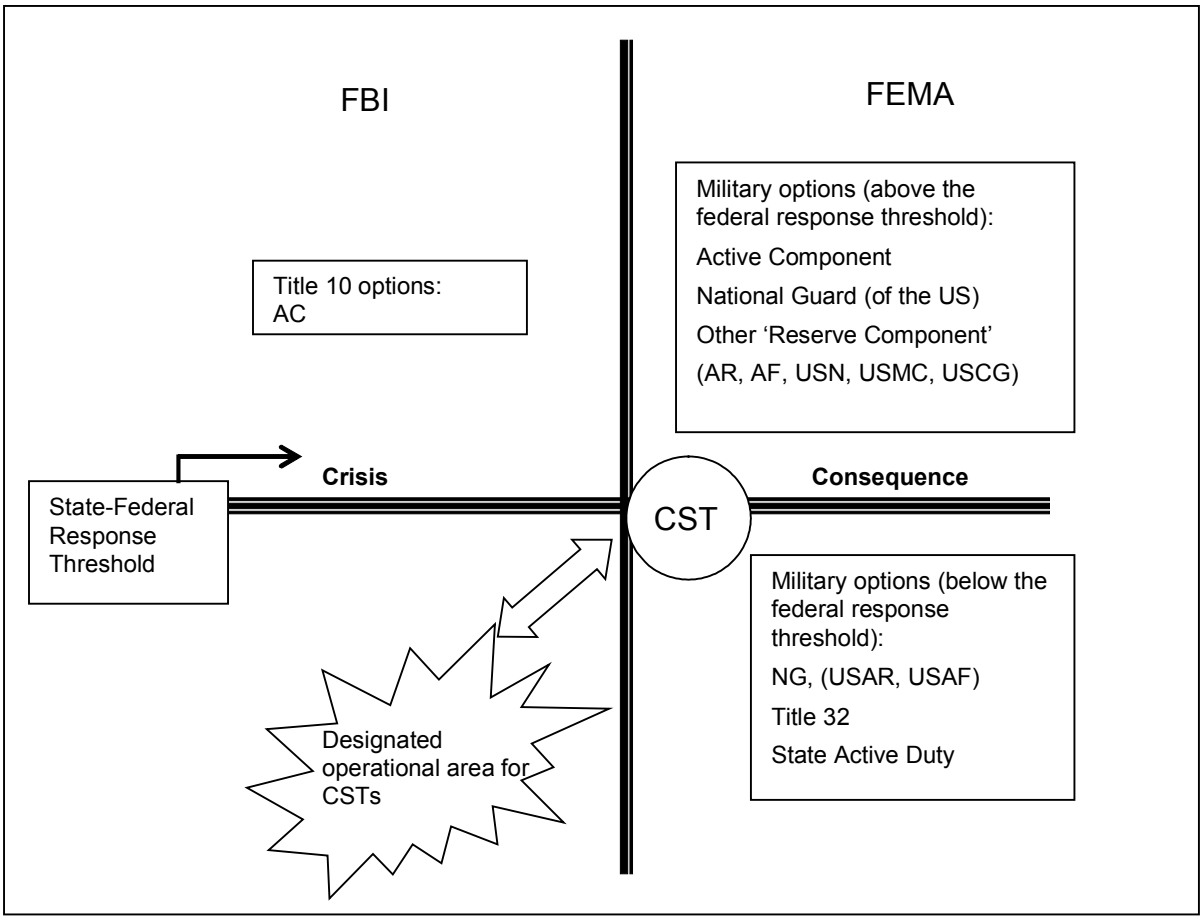

Figure 1-1. Consequence Management, DOD Response Options

broken down into six smaller sections—command, operations, communications, administration and logistics (A&L), medical, and survey—that have been trained and equipped to provide a technical capability to "reach back" to other experts who can assist the incident commander (IC). These teams provide a unique military capability. They can deploy rapidly to a suspected or actual terrorist attack, conduct reconnaissance to determine the effects of the attack, provide situational understanding, provide technical consultation to local authorities on the effects of the attack to minimize the impact, and facilitate follow-on military support through validated civilian requests for assistance. CST deployment and operations are also supported through the use of checklists and timely reporting (see Appendixes D and E).

CAPABILITIES

1-7. The CST provides assessments and presumptive identification to analyze most CBRNE agents and substances. The CST sophisticated detection, analytical, and protective equipment allows for operations to take place in environments that contain many different TIM and CBRNE materials. The personal-protective equipment (PPE) used by CSTs provides more extensive protection (such as Occupational Safety and Health Administration [OSHA] Levels A and B) from hazardous material (HAZMAT) than does the

equipment used by most military units. (Mission-oriented protective posture [MOPP] 4 is the approximate equivalent of OSHA Level C protection.)

1-8. CSTs have a unique ability to asssess CBRNE events. This is accomplished through the expertise of personnel and the use of several computer-based modeling programs. In addition, the survey and medical team's high state of training and advanced technology equipment allow for accurate and timely sample collection and identification of CBRNE agents and substances. The CST also provides the ability to act as a CBRNE reconnaissance force that can provide a unique view at the incident site.

1-9. The assessment process also supports deliberate and crisis action planning. For example, see Appendix F for a sample CST operations plan (OPLAN) and warning order (WO). Assessments include the use of intelligence preparation of the battlespace (IPB) techniques to determine posssible adversary COAs. Capabilities and needs assessments also occur to determine what capabilities are needed to support the required response actions. Assessments occur prior to, during, and after an incident. Assessment is an ongoing process that is undertaken to help ensure the safety of personnel and the preservation of property.

1-10. The CST advises the ICs and emergency responders. For example, during exercises and training, the CST can advise leaders and first responders on the hazards and countermeasures associated with a response to a CBRNE incident. During such a response, a CST can recommend measures such as the follow-on capabilities (such as types of units, equipment, and supplies) needed to support mitigation measures at an incident site. Postincident, the CST can advise on measures such as the preparation of a transition plan. This plan helps support the disengagement of military units for redeployment to home stations. The CST state and federal technical reach-back capability enables the commander to obtain subject matter expertise on CBRNE matters and provide situational awareness (SA) to appropriate agencies not at the incident site. See Appendix G for sample reach-back capabilities that could be used to support CST operations.

1-11. The CST assists leaders and emergency responders by providing a capability to coordinate and conduct liaison, if requested, with other response assets. The CST assists the IC in formulating and communicating appropriate requests for additional support. The CST may also provide recommendations on how to integrate the use of follow-on CBRNE response assets.

THREAT

1-12. The traditional view of CBRNE has evolved with the proliferation of improvised CBRNE devices. We have moved into an era where these types of weapons are no longer limited to the purview of typical superpower nations. The technology to produce improvised CBRNE agents continues to spread. The ability to weaponize these agents can also be accomplished by simple (placing anthrax spores in an envelope) or sophisticated (using spray or a bursting device to disseminate TIM) means.

CHEMICAL WEAPONS

1-13. Chemical weapons are generally defined as toxic chemicals and their precursors, except when intended for a purpose not prohibited under the Chemical Weapons Convention (CWC); a munition or device designed to cause death or other harm through toxic properties; or any equipment specifically designed for use directly in connection with the employment of munitions or devices.

1-14. Chemical agents are also generally grouped according to the potential severity of their effects—lethal and incapacitating agents. Lethal chemical agents are designed to kill or severely injure. Incapacitating agents are chemical substances that are intended to kill, seriously injure, or incapacitate personnel through their physiological effects. Chemical agents can cause psychological and physiological effects. They can cause contamination or damage that will restrict the use of facilities and/or equipment and supplies.

1-15. Chemical compounds such as riot control agents (RCAs) can also be used. To support assessments, see FM 3-11.9 for detailed information on chemical agents. Another key reference is FM 8-285.

Nerve Agents

1-16. Nerve agents, such as tabun and sarin, are generally clear and colorless liquids. These primarily organophosphorus compounds may be absorbed through the skin or inhaled through the respiratory tract. Exposure to a nerve agent may cause widespread systemic effects (such as respiratory failure) and/or death within minutes.

Blood Agents

1-17. Blood agents, such as hydrogen cyanide and cyanogen chloride, are generally colorless liquids widely used in commercial chemical manufacturing. Blood agents interfere with the exchange of oxygen with the cells of the body. These agents enter the body through the respiratory system and act quickly, if inhaled in sufficient quantities. Even though blood agents are fast-acting, they dissipate quickly.

Choking Agents

1-18. Choking agents, such as phosgene and diphosgene, are generally clear and colorless and are highly volatile liquids. Choking agents attack lung tissue and interfere with the exchange of oxygen within the lungs. These agents enter the body through the repiratory system and, if inhaled, act almost immediately. They also cause damage to the eyes.

Blister Agents

1-19. Blister agents, such as mustard, are generally yellow-to-brown, oily substances. The vapor may be colorless with a slight garlic- or mustard-like odor. Blister agents are absorbed through the skin or eyes or inhaled through the respiratory tract. Blister agents burn and blister the skin and will generally persist for hours to days.

BIOLOGICAL WEAPONS

1-20. Biological weapons are materials that project, disperse, or disseminate a biological agent, including anthropod vectors. A biological agent is a microorganism that causes disease in personnel, plants, or animals or causes the deterioration of material. Biological agents can cause psychological and physiological effects. They can cause contamination or damage that will restrict the use of facilities and impact the economy.

1-21. One of the dangers of biological weapons is amplified by the fact that exposure to the agents would probably not be diagnosed until symptoms appear. Personal protection generally consists of individual protection and medical measures (such as immunization) or the application of some other postincident medical treatment (such as antibiotics).

1-22. Biological-agent dissemination could be accomplished by such measures as aerosol dissemination or by the use of vectors or bursting devices. Biological agents can be produced in the laboratory or purchased from a number of medical research firms.

1-23. Biological agents include bacteria, viruses, rickettsias, and toxins. These agents can be weaponized to project, disperse, or disseminate biological agents. To support assessments, see FM 3-11.9 for detailed information on biological agents. Another key reference is FM 8-284.

- Bacteria are defined as single-celled, microscopic, plant-like organisms. A possible bacterial agent of concern could include anthrax. A biological warfare (BW) attack with anthrax would probably be delivered by aerosol. Following an incubation period, anthrax affects an individual's respiratory system; and the fatality rate is high following the onset of pulmonary symptom
- Viruses are defined as parasitic organisms that live in the cells of their selected hosts. A possible viral agent of concern includes smallpox. Smallpox can also be delivered as an aerosol. Following an incubation period, smallpox has a high fatality rate and is transmissible from man to man.
- Rickettsias are defined as intracellular, parasitic microorganisms that are intermediate in size between the bacteria and viruses. A possible rickettsia agent of concern could include Rocky Mountain Spotted Fever. Rocky Mountain Spotted Fever can be delivered as an aerosol and has a high fatality rate. The rickettsia agents are not transmissible from man to man.
- Toxins are defined as poisonous substances produced by microorganisms, plants, or animals. A possible toxin of concern includes botulinum.

RADIOLOGICAL WEAPONS

1-24. Radiological materials are used in many industrial and medical occupations and could be readily available to terrorists. Dispersal could occur through the use of radiological-dispersal devices or through simple radiological dispersal. A radiological-dispersal device could be any explosive device intended to spread radioactive material upon detonation and cause physiological or psychological effects or material contamination. As such, they

do not produce the massive blast and thermal effects that are produced by a nuclear detonation. A terrorist could wrap an improvised explosive device (IED) with radiological materials to create an incident in which the initial explosion may kill or injure persons in the immediate vicinity of the device. Following the incident, the possible ingestion and inhalation of the radioactive particles would pose a health risk. Simple radiological dispersal is an act intended to spread radioactive material not involving an explosive device. A terrorist need only disperse radiological material (such as gamma, beta, or alpha emitters) secured from a medical laboratory, industrial plant, or other site.

NUCLEAR WEAPONS

1-25. While the detonation of a nuclear device is perhaps the least likely scenario for a terrorist incident, it has the potential to cause the greatest damage. Effects of a nuclear detonation include thermal, blast, and nuclear radiation.

1-26. Thermal radiation consists of heat and light and results from the nuclear detonation. Thermal radiation can cause widespread injuries in the form of skin burns and retinal damage (flash blindness). Thermal radiation can also cause fires or damage or destroy heat-sensitive and optical systems. The type of weapons burst (air, surface, or subsurface) and the atmospheric conditions influence both the range and intensity of thermal damage.

1-27. Blast effects consist of shock waves, high overpressure, and severe winds that can demolish buildings, destroy equipment, and uproot trees. Though the shock front achieves sufficient strength to devastate most land features, the type of nuclear burst limits the severity of destruction. Blast is not an instantaneous effect. A finite amount of time will elapse between the flash and the arrival of the shock wave relative to a person's distance from the point of detonation (ground zero).

1-28. Nuclear radiation is the most widespread and longest lasting weapons effect that comes from the emission of radioactive products (gamma, beta, and alpha radiation). These appear in two forms: initial and residual radiation. Initial radiation emitted during the first minute after detonation produces deadly gamma rays and neutrons. Residual radiation is the most prevalent in ground bursts. Other nuclear-weapons effects include electromagnetic pulse that can disrupt radio communications and damage electronic equipment. Characteristics of nuclear radiation products include the following.

- Gamma ray radiation is high-energy, electromagnetic radiation emitted by nuclei during nuclear reactions or radioactive decay. These rays have high energy and a short wave length. Gamma rays are potentially lethal to humans, depending on the intensity of the flux.
- Beta radiation is an electron or positron emitted by an atomic nucleus during radioactive decay. Beta radiation can be lethal, depending on the dose and time of exposure; it is easily shielded by aluminum.
- Alpha radiation is a positively charged particle made up of two neutrons and two protons emitted by certain radioactive nuclei.

Alpha radiation can be stopped by light materials (such as a sheet of paper) and pose no direct external radiation threat; however, they can pose a serious health threat if ingested.

1-29. To help support assessments, see FM 4-02.283 for more information on the effects of radiological and nuclear weapons.

TOXIC INDUSTRIAL MATERIAL

1-30. TIMs are substances that may create signs and symptoms similar to nuclear, biological, and chemical (NBC) exposure. These materials are found throughout the normal transaction of daily business in the US and are transported on our railways, roadways, and waterways. They may or may not be precursors to CBRNE agents. Most of the materials contain volatile organic compounds (VOCs), which are materials that contain hydrocarbons and possibly other hazardous elements. They may be naturally occurring or man-made and may evaporate easily based on agent characteristics. Testing has proven that extended exposure to such materials may lead to debilitating injury. Some are carcinogenic (such as benzene) or mutagenic (such as hexane).

TERRORISM

1-31. Technological innovations and the widening proliferation of CBRNE hardware and scientific expertise increase the likelihood that states, nonstate actors, or transnational groups could threaten the US homeland and population directly and, in times of conflict, deny US access to critical overseas and domestic infrastructure. Terrorism remains one of the deadliest and most persistent threats to US security. The motives, perpetrators, and methods of terrorist groups are evolving in ways that complicate analysis, collection, and counteraction; and they require the ability to respond flexibly and quickly. The rise of a new breed of terrorist, such as Osama bin Laden, who is interested in inflicting mass death and destruction, does not bode well for the future security of US interests. These groups can strike anytime and anywhere, and they are spurred by seemingly unrelated events for which they blame the US. They have a widening global reach and a high degree of proficiency with more sophisticated weapons and tactics.

1-32. There are different definitions of terrorism, and CST leaders remain aware of the different meanings. For example, the terrorism definition as defined in Joint Publication (JP) 1-02 states that terrorism is “the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.” However, per the Federal Response Plan (FRP), the Federal Bureau of Investigation (FBI) defines a terrorist incident as “a violent act, or an act dangerous to human life, in violation of the criminal laws of the US or of any state, to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.”

CATEGORIES OF TERRORIST GROUPS

1-33. Terrorists are either non-state-supported (indigenous or transnational), state-supported, or state directed. Non-state-supported terrorist groups are autonomous and receive no significant support from a government. State-supported groups generally operate independently but receive support from one or more governments. This support may include weapons, training, money, intelligence, or safe havens. State-directed terrorist organizations act as agents of a government. Such groups receive intelligence, logistics, and operational support from the sponsoring government, frequently through diplomatic missions.

1-34. Terrorism can be a relatively inexpensive method of carrying out attacks against an enemy or its interests and is potentially deniable. Those who spawn and foster terrorist activities are becoming increasingly sophisticated in obtaining and transferring financial support and in planning future terrorist attacks. CBRNE devices could be employed in future attacks with devastating results. The specific target could include the general public and/or emergency first responders (EFR). Local, state, and federal law enforcement officials monitor suspected terrorist groups and try to prevent or protect against a suspected attack. Additionally, the USG works with other countries to limit the transfer of WMD technologies and sources of support for terrorism.

TERRORIST TACTICS

1-35. A terrorist attack can take several forms, depending on the technological means available to the terrorist, the nature of the political issue motivating the attack, and the points of weakness of the terrorist's target. Bombings are the most frequently used terrorist method in the US. Other possibilities include attacks on transportation facilities and attacks against utilities or other public services.

1-36. The basic types of tactics that terrorist groups can employ include hijackings, kidnappings, bombings, assassinations, armed assaults, and barricade hostage incidents. Objectives and organizational capabilities of a group dictate the tactics it uses. Terrorist groups typically use hijackings, kidnappings, and barricade hostage incidents when the group wishes to force the targeted company or government into negotiations.

1-37. Such incidents increase the level of risk to the terrorist organization and require a mature planning, operations, logistics, and intelligence capability to successfully conduct the operations. Bombings, assassinations, and armed assaults are less risky and generally require less organizational capabilities. These tactics tend to be used to accomplish the following goals:

- Create a climate of fear in a targeted group or nation through a sustained campaign of violence (such as the forwarding of anthrax-laden mail parcels that contaminated US government and corporation facilities and caused fatalities and fear among the general public and government workers).
- Retaliate for previous incidents or situations affecting the terrorist organization or its causes (such as the terrorist assertion that the

destruction of the World Trade Center was revenge because of the presence of US armed forces in the Middle East).

- Degrade or disrupt capabilities that adversely affect terrorist interests (such as Al Qaeda's anticipation that attacks against targets such as the Pentagon and New York City would reduce America's economic power and encourage an "America first" siege mentality and a retreat from foreign commitments critical to our nation's security).
- Eliminate specific individuals or groups (such as BW agent [anthrax] attack against members of US Congress in 2001).

1-38. To attain their goals, terrorist organizations depend on receiving adequate information for planning and executing an operation. Operations security (OPSEC) denies terrorist organizations the information they require for planning. The following paragraphs discuss the terrorist threat to the US and the role of sponsoring nations and terrorist organizations in executing attacks.

TERRORIST OBJECTIVES

1-39. Terrorists intend their activities to have an emotional impact on the target audience, causing it to act in a manner that furthers the group's objectives. Terrorist operations generally are categorized in terms of their associated goals. These goals traditionally could include recognition, coercion, intimidation, provocation, and insurgency support. Early in their life span, terrorist groups often carry out attacks designed to gain recognition. The objective of these attacks may be national and/or international attention for the group and its stated objectives. Groups often mount such attacks that may involve protracted hostage seizures against highly visible symbols of state control (such as national airlines). Groups may use coersion to force individuals, organizations, or governments to act in a desired manner. Using this strategy, terrorists selectively target facilities with the intent of bringing increasing pressure to bear on the targeted activity. Terrorist attacks designed to intimidate are a means of preventing organizations or governments from acting in a defined manner. These attacks could also be launched against critical infrastructures, popular or high profile individuals, or important facilities.

RECOGNIZING A TERRORIST ATTACK

1-40. Recognizing suspicious incidents may be difficult, but units and applicable personnel are being extremely alert to clues and their surroundings. Occupancy location, the type of event, timing of the event, and on-scene warning signs also provide indicators of terrorist activity.

Occupancy or Location

1-41. Symbolic and historical targets include those that represent some organization or event that is particularly offensive in the minds of extremists. These targets are often government-related.

1-42. Public buildings or assembly areas provide the opportunity to cause mass casualties. Some of these public buildings are also symbolic targets, so the terrorist can cause massive casualties and link the owner/operator of the

building or assembly area with danger in the minds of the public. Examples include shopping malls, convention centers, entertainment venues, and tourist destinations.

1-43. Some businesses may conduct operations that are regarded as controversial, and these enterprises may draw the attention of terrorist groups. Abortion clinics, nuclear facilities, and furriers all fall into this category.

1-44. Infrastructure systems include those operations that are necessary for the continued functioning of our society. Major cities contain targets such as power plants, phone companies, water treatment plants, mass transit, and hospitals. Attacks on any of these targets have the potential to disrupt entire regions.

Type of Event

1-45. Certain types of events raise the awareness of possible terrorism involvement. Explosions and/or incendiaries are among the most often used weapons by terrorists. Any bombing or suspicious fire may signify terrorist involvement, especially when combined with location or occupancy factors. Incidents involving firearms are always treated as suspicious.

Timing of the Event

1-46. Government facilities may operate at heightened states of security awareness on significant dates such as April 19. This date is the anniversary of both the fire at the Branch Davidian compound in Waco, Texas, and the bombing of the Alfred P. Murrah building in Oklahoma City, and so has become a rallying point for antigovernment extremists. Events that occur on specific days of the week and times are worth treating with suspicion.

On-scene Warning Signs

1-47. On-scene warning signs should always be evaluated for indications that one is dealing with a suspicious incident. Unexplained patterns of illness or deaths can be due to chemical and biological (CB) agents. Some of these substances have recognizable odors and/or tastes. Unexplained signs and symptoms of skin, eye, or airway irritation may be due to chemical contamination, as can unexplained vapor clouds, mists, and plumes. Personnel should keep on the lookout for chemical containers, spray devices, or lab equipment in unusual locations. They should also watch for items or containers that appear out of place or unusual which might indicate a secondary device. Spot fires or fires of unusual behavior may also arouse one's suspicions, as can anything that appears not "normal" for a given incident scene. Indicators of a terrorist CBRNE attack could include—

- Anonymous tips, phone calls, or notes of a threatening nature that may identify groups or carry extremist messages.
- Surveillance of suspicious persons by federal offices or federal employees performing official duties.
- Unidentified or unattended packages, cans, or other containers left in or near government offices.

- Unattended and unoccupied vehicles parked in unauthorized or inappropriate locations, particularly those in proximity to buildings or other structures.
- Requests for plans, blueprints, or engineering specifications for federal buildings or commercially owned buildings that house government offices by those who have no official reason to have them.
- Unauthorized access to unsecured areas by unknown or unidentified persons who have no apparent reason for being there.
- Packages or heavy envelopes (often without a legible return address) that arrive in the mail from unknown senders or that have a peculiar odor or appearance.
- Confrontation with angry, aggressive, belligerent, or threatening persons by federal officials in the performance of their official duties.
- Extreme threats or violent behavior by coworkers who indicate that they may resort to revenge against a group, company, or government agency.